POWER ALLOCATION, RELAY SELECTION & COOPERATIVE TECHNIQUES FOR PHYSICAL LAYER SECURITY IN RELAYED COMMUNICATION SYSTEMS

SARBANI GHOSE

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI

April, 2017

POWER ALLOCATION, RELAY SELECTION & COOPERATIVE TECHNIQUES FOR PHYSICAL LAYER SECURITY IN RELAYED COMMUNICATION SYSTEMS

by

SARBANI GHOSE

Department of Electrical Engineering

Submitted

in fulfillment of the requirements of the degree of **Doctor of Philosophy**

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

APRIL, 2017

Certificate

This is to certify that the thesis entitled **"Power Allocation, Relay Selection & Cooperative Techniques for Physical Layer Security in Relayed Communication Systems"** being submitted by **Ms. Sarbani Ghose** to the Department of Electrical Engineering, Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy**, is the record of the bona-fide research work carried out by her under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted either in part or in full to any other university or institute for the award of any degree or diploma.

Date:

Place:

(Dr. Ranjan Bose)
Professor
Department of Electrical Engineering
Indian Institute of Technology Delhi
Hauz Khas, New Delhi 110016

Acknowledgements

To start with, I wish to express my deep gratitude to my supervisor Professor Ranjan Bose. He has been a source of constant encouragement and always gave me the best support. He instilled into me the motivation for learning the new techniques and the unique methodologies to keep oneself abreast of the latest technological developments in the fast growing scenario. I am deeply indebted to my student research committee members Professors Manav Bhatnagar, Vinay Joseph Ribeiro, and Brejesh Lall, for many a useful interactions and for their kind comments and suggestions which were always useful and fulfilling.

I gratefully acknowledge all the expert guidance from the professors at the IIT Delhi from whom I have benefited a lot during the courses. I offer my regards to all members of the Research Scholar Lab, who supported me in all respect during the completion of the Ph.D. Most importantly, my heartfelt gratitude is for my father Sudipta Ghose who always supported me in all my academic pursuits and encouraged me to do my best. I would also like to thank my husband Anirban Kundu for his unflinching support and loving encouragement.

Sarbani Ghose

Abstract

Wireless networks are broadcast in nature. Hence wireless transmission can be heard by multiple receivers with different signal strengths. With the help of a 'friendly jammer', we can create confusion at the eavesdropper. That brings us to a design problem, that is how to fulfill rate requirement of secure communication with a constraint on the resources i.e. the transmit power. In this thesis, we first propose how to design optimal weight at the friendly jammer such that the overall secrecy rate is maximized, under the constraint of total power. We obtain expressions for optimal source power that maximizes secrecy rate. We find that beyond a region, it is better to rely on direct transmission and within the region jamming is effective. We term this region as 'effective region for jamming'. Similar region is found when we aim at minimizing total transmit power, with a constraint on secrecy rate. It is observed that the secrecy rate improves in a less cluttered environment. After inclusion of the fading model, it is observed that the secrecy rate improves, for two particular cases i.e. mobile eavesdropper and mobile jammer. Thus, fading helps to improve secrecy.

Relaying can expand the coverage area of communication and offer diversity gains. With the help of a relay, a positive secrecy capacity can be achieved which is otherwise zero when relay is not being used. Next, we propose an adaptive scheme that combines the merits of both decode-and-forward (DF) and amplify-and-forward (AF) scheme. If the signal-to-noise ratio (SNR) of first hop is below a certain prescribed threshold, then AF is adopted and beyond a threshold DF is employed. We find that at low secrecy rate, to achieve same secrecy performance

hybrid decode-and-forward (HDAF) requires higher SNR as compared to the case of higher secrecy rate. A fixed 'least secrecy outage' is obtained depending on input parameters. When the destination and eavesdropper both employ maximal ratio combining (MRC) receiver, we have derived a closed-form expression for secrecy outage probability (SOP) of this system. Also asymptotic performance of HDAF scheme is obtained. It is seen that the effect on unbalance is more pronounced at lower secrecy rate as compared to higher rate.

Secrecy capacity can be improved by selecting a single relay that ensures best transmission link to the destination and worst link to the wiretapper. Considering a network with multiple AF relays, we solve joint power allocation and optimal relay selection problem. When source transmits message signal, destination sends jamming signal concurrently. Closed-form expression of SOP of an optimal relay selection based on destination jamming has been derived. Relay selection schemes are formulated based on instantaneous, statistical channel state information (CSI) of the eavesdropper. It has been seen secrecy outage is worst when relay selection is performed without taking into account jamming, in the presence of eavesdropper.

In a multi-node relaying network, the intended channel quality can be enhanced through the collaboration of relays, which exploits the spatial diversity by relays at the transmitter and/or the receiver. Multiple relays can cooperate to combine redundant copies of the same signal, hence achieve a diversity gain. In this thesis, we analyze the secrecy performance of a single relay-based dual-hop communication systems with diversity combining a) at the eavesdropper only, b) at the destination and the eavesdropper. We find that secrecy performance is the best, when the relay is able to decode the message perfectly. It is observed that the availability of channel state information (CSI) can only help to improve secrecy when secrecy rate is low. It is also observed that unbalances created by imposing constraint on either of the source-relay or relay-destination average SNR does not yield similar performance.

सार

वायरलेस नेटवर्क प्रकृति में प्रसारित किए जाते हैं। इसलिए बेतार संचरण अलग सिग्नल क्षमताओं के साथ कई रिसीवर से सुना जा सकता है। एक `अनुकूल जैमर 'की मदद से, हम छिपकर बातें सुनेवाला पर भ्रम की स्थिति पैदा कर सकते हैं। यही कारण है कि एक डिजाइन समस्या के लिए हमें लाता है, कि एक बाधा के साथ सुरक्षित संचार की दर की आवश्यकता को पूरा करने के लिए कैसे संसाधनों अर्थात संचारित शक्ति पर है। इस शोध में, हम पहले प्रस्ताव कैसे अनुकूल जैमर पर इष्टतम वजन डिजाइन करने के लिए इस तरह के हैं कि समग्र गोपनीयता दर बड़ा किया गया है कुल बिजली की कमी के तहत,। हम इष्टतम स्रोत शक्ति है कि गोपनीयता दर अधिकतम के लिए अभिव्यक्ति प्राप्त करते हैं। हम पाते हैं कि एक क्षेत्र से बाहर है, यह सीधा प्रसारण पर और भीतर क्षेत्र ठेला प्रभावी है भरोसा करने के लिए बेहतर है। हम `प्रभावी रूप से इस क्षेत्र में पद ठेला के लिए इस क्षेत्र '। जब हम गोपनीयता दर पर एक बाधा के साथ, कुल संचारित शक्ति को कम करने का उद्देश्य इसी प्रकार क्षेत्र पाया जाता है। यह देखा गया है कि गोपनीयता दर अव्यवस्था कम वातावरण में सुधार। फडिंग मॉडल के शामिल किए जाने के बाद, यह पाया गया है कि गोपनीयता दर, बेहतर बनाता है दो विशेष मामलों मोबाइल छिपकर बातें सुनेवाला और मोबाइल जैमर अर्थात्। इस प्रकार, लुप्त होती गोपनीयता सुधार करने के लिए मदद करता है।

प्रसारण संचार के कवरेज क्षेत्र का विस्तार और विविधता लाभ की पेशकश कर सकते हैं। एक रिले की मदद से, एक सकारात्मक गोपनीयता क्षमता प्राप्त किया जा सकता है जो अन्यथा शून्य है जब रिले का उपयोग नहीं किया जा रहा है। इसके बाद, हम एक अनुकूली योजना है कि दोनों डिकोड-एंड-फॉरवर्ड (डीफ) और एम्पलीफी-एंड-फॉरवर्ड (आफ) योजना की खूबियों को जोड़ती प्रस्ताव करते हैं। संकेत से शोर अनुपात (असनर) पहले हॉप की एक निश्चित निर्धारित सीमा से नीचे है, तो वायुसेना अपनाया है और एक सीमा से परे डीफ कार्यरत है। हम कम गोपनीयता दर पर, प्राप्त करने के लिए है कि एक ही गोपनीयता प्रदर्शन संकर डिकोड-एंड-फॉरवर्ड (अच्डीफ) उच्च असनर की आवश्यकता है उच्च गोपनीयता दर के मामले की तुलना में पाते हैं। एक निश्चित `कम से कम गोपनीयता आउटेज' इनपुट पैरामीटर के आधार पर प्राप्त की है। गंतव्य और छिपकर बातें सुनेवाला दोनों अधिक से अधिक अनुपात को रोजगार जब संयोजन (एमआरसी) रिसीवर, हम इस प्रणाली की गोपनीयता आउटेज संभावना (एसओपी) के लिए एक पूर्ण-सूत्र अभिव्यक्ति ली गई है। इसके अलावा अच्डीफ योजना के असिम्प्टोटिक प्रदर्शन प्राप्त की है। यह देखा गया है कि असंतुलित पर प्रभाव कम गोपनीयता दर से और अधिक स्पष्ट उच्च दर की तुलना में है।

गोपनीयता क्षमता एक भी रिले कि गंतव्य के लिए सबसे अच्छा ट्रांसमिशन लिंक और छिपकर बातें सुनेवाला लिए सबसे खराब लिंक सुनिश्चित करता है का चयन करके सुधार किया जा सकता। कई वायुसेना रिले के साथ एक नेटवर्क को देखते हुए, हम संयुक्त शक्ति आवंटन और इष्टतम रिले चयन समस्या का समाधान। स्रोत संदेश संकेत पहुंचाता है, गंतव्य समवर्ती संकेत जाम भेजती है। गंतव्य ठेला के आधार पर एक इष्टतम रिले चयन के एसओपी का पूर्ण-सूत्र अभिव्यक्ति प्राप्त किया गया है। रिले चयन योजनाओं छिपकर बातें सुनेवाला की तात्कालिक, सांख्यिकीय चैनल राज्य सूचना (सीएसआई) के आधार पर तैयार की जाती हैं। यह देखा गया है गोपनीयता आउटेज सबसे खराब जब रिले चयन छिपकर बातें सुनेवाला की उपस्थिति में, खाते ठेला में लेने के बिना किया जाता है |

एक बहु नोड रिले नेटवर्क में, इरादा चैनल गुणवत्ता रिले का सहयोग है, जो ट्रांसमीटर और / या रिसीवर पर रिले द्वारा स्थानिक विविधता कारनामे के माध्यम से बढ़ाया जा सकता है। एकाधिक रिले एक ही संकेत की अनावश्यक प्रतियां गठबंधन है, इसलिए एक विविधता लाभ प्राप्त करने में सहयोग कर सकते हैं। इस शोध में, हम विविधता गंतव्य और छिपकर बातें सुनेवाला पर छिपकर बातें सुनेवाला केवल, ख) में एक संयोजन) के साथ एक एकल रिले-आधारित दोहरे हॉप संचार प्रणाली की गोपनीयता के प्रदर्शन का विश्लेषण। हम पाते हैं कि गोपनीयता प्रदर्शन, सबसे अच्छा है जब रिले पूरी तरह से संदेश को डिकोड करने में सक्षम है। यह देखा गया है कि चैनल राज्य सूचना (सीएसआई) की उपलब्धता केवल गोपनीयता बेहतर बनाने में मदद कर सकते हैं जब गोपनीयता दर कम है। यह भी देखा गया है कि स्रोत-रिले या रिले-गंतव्य औसत असनर में से किसी पर बाधा भव्य इसी तरह के प्रदर्शन की उपज नहीं है के द्वारा बनाई गई असंतुलन कि।

Contents

List of Figures

List of Tables

List of Abbreviations

AF	Amplify-and-Forward
AN	Artificial Noise
AS	Asymptotic
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPCU	Bits Per Channel Use
CCI	Co-Channel Interference
CJ	Cooperative Jamming
CR	Cognitive Radio
CS	Conventional Selection
CS-J	Conventional Selection with Jamming
CS-NJ	Conventional Selection without Jamming
CSI	Channel State Information
DAF	Decode-Amplify-and-Forward
dB	Decibel
DF	Decode-and-Forward
DSC	Distributed Selection Combining
DSSC	Distributed Switch-and-Stay Combining
EGC	Equal Gain Combining
ERFR	Effective Region For Relaying
ESR	Ergodic Secrecy Rate
GSVD	Generalised Singular Value Decomposition
HDAF	Hybrid Decode-Amplify-and-Forward
IID	Independent and Identically Distributed
INID	Independent and Not Identically Distributed
IoT	Internet of Things

Table 1 – *Continued from previous page*

ISI	Inter Symbol Interference
LOS	Line-of-Sight
MGF	Moment Generating Function
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MMSE	Minimum Mean Square Error
MRC	Maximal Ratio Combining
MRT	Maximal Ratio Transmission
NF	Noise Forwarding
NOD	NO Direct link available
OFDMA	Orthogonal Frequency Division Multiple Access
OS	Optimal Selection
OSI	Open Systems Interconnection
PDF	Probability Density Function
PLE	Path Loss Exponent
PLS	Physical Layer Security
QoS	Quality of Service
RV	Random Variable
SC	Selection Combining
SDC	Selection Diversity Combining
SER	Symbol Error Rate
SISO	Single-Input Single-Output
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
SRM	Secrecy Rate Maximization
SS	Suboptimal Selection
STBC	Space Time Block Code
TC	Threshold Combining

Table 1 – *Continued from previous page*

TH	Threshold
TPM	Transmit Power Minimization
ZF	Zero Forcing